PATENT ABSTRACTS OF JAPAN

(11)Publication number : **04-195383**
(43)Date of publication of application : **15.07.1992**

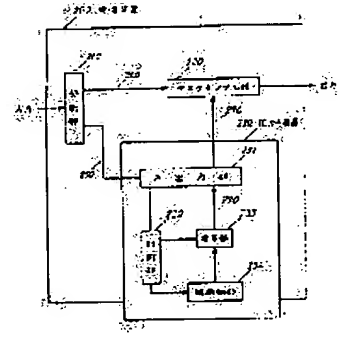
(51)Int.CI. G06K 19/073
B42D 15/10

(21)Application number : **02-328713**
(22)Date of filing : **27.11.1990**

(71)Applicant : **MATSUSHITA ELECTRIC IND CO LTD**
(72)Inventor : **MUTO YOSHIHIRO**
TAKAGI SHINYA

(54) IC CARD DEVICE AND RECEIVER USING THE SAME

(57)Abstract:
PURPOSE: To completely protect secret information by providing a RAM for storing the secret information and an auxiliary power source for the RAM in the IC card device and further providing a means which stops supplying electric power to said RAM when an illegal action is taken.
CONSTITUTION: The receiver 200 uses the IC card device 230 and broadcast data are divided by a division part 210 into secret data 250 and sent data 260. The secret data 250 is sent the IC card device 230 with a key parameter. A control part 232 deciphers a key parameter for descrambling the sent data 260 by using the key parameter and the master key of a key storage part 234. A descrambling part descrambles the sent data 260 with the key parameters 270 and outputted the resulting data finally. The RAM stored with the secret information for key deciphering and the power source are connected by a lead line laid around in the IC card device 100 and when this RAM is taken out, the lead wire is broken.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of

rejection]
[Date of requesting appeal against examiner's decision of rejection]
[Date of extinction of right]

⑲日本国特許庁（JP）　⑪特許出願公開

⑫公開特許公報（A）　平4－195383

⑤1Int. Cl.⁵	識別記号	庁内整理番号	⑬公開　平成4年(1992)7月15日
G 06 K 19/073			
B 42 D 15/10	521	9111－2C	
		6711－5L　G 06 K 19/00　P	

審査請求　未請求　請求項の数 2　（全5頁）

⑤4発明の名称　ＩＣカード装置およびそれを用いた受信装置

⑳特　願　平2－328713

㉒出　願　平2(1990)11月27日

⑦2発 明 者　武藤　義弘　大阪府門真市大字門真1006番地　松下電器産業株式会社内

⑦2発 明 者　高木　伸哉　大阪府門真市大字門真1006番地　松下電器産業株式会社内

⑦1出 願 人　松下電器産業株式会社　大阪府門真市大字門真1006番地

⑦4代 理 人　弁理士 小鍛治 明　外2名

明　細　書

1. 発明の名称

ＩＣカード装置およびそれを用いた受信装置

2. 特許請求の範囲

（1）ＣＰＵと、外部からのコマンドに従った処理を行うためのプログラムを格納するＲＯＭと、機密情報を格納するＲＡＭと、前記ＲＡＭ内のデータを保持するための電源を供給する補助電源と、不正行為が行われた場合に前記ＲＡＭへの電源の供給を停止する電源供給遮断手段とを有することを特徴とするＩＣカード装置。

（2）請求項1に記載のＩＣカード装置が接続された受信装置であって、受信したデータを機密データと通信相手に伝達すべき所望の伝送データとに分割するデータ分割部と、前記機密データから解読鍵を生成する復号部と、前記復号部を作動させるためのマスター鍵を格納している鍵格納部と、生成された前記解読鍵を用いて前記伝送データをデスクランブルするデスクランブル部とから構成され、少なくとも前記鍵格納部が前記ＩＣカード装置上に存在することを特徴とする受信装置。

3. 発明の詳細な説明

産業上の利用分野

本発明は、ＩＣカード装置に関するもの、および衛生放送、ケーブルテレビなどの通信において、暗号化された通信データを一定のアルゴリズムに従ってデスクランブルする事の許可をＩＣカード装置によって与える受信装置に関するものである。

従来の技術

放送受信方式において、受信者を限定した通信を行うために、契約時にＩＣカード装置内のＲＯＭあるいは書換え可能な不揮発性メモリ（以下ＥＰＲＯＭと呼ぶ）に秘密情報を格納して発行し、ＩＣカード装置を所持している人にのみ受信を許可し、許可されていないもの（具体的には料金未納のもの等）の受信を不可能にしている。

第3図にＩＣカード装置を用いた従来技術の放送受信方式（特開昭62－180625号公報）の基本構成を示す。この放送受信方式はアナログ放送を基本としている。この放送受信方式におい

て、ＩＣカード装置３３０は受信装置３００から復調されディジタル化された信号を入力データとし、入出力部３３１を通してデスクランブラ則３２０にデータに引き渡す。デスクランブラ則３２０は放送センター等に管理されており、予め秘密のプログラムとしてＩＣカード装置３３０内の書換え可能なメモリに格納されている。デスクランブラ則３２０はカウンタあるいはタイマ等を利用した制御部３３２によって制御されている。デスクランブルされたデータは再び入出力部３３１を通して受信装置３００に出力される。このように、データを復元するデスクランブラ則がＩＣカード装置内に格納され、ＩＣカード装置を所持している人にのみ放送の受信を許可することを特徴としていた。

発明が解決しようとする課題

デスクランブラ則を長時間変えないでおくと、信号の性質を解析するなどの方法でデスクランブラ則が知られてしまう可能性があり、また、従来技術のＩＣカード装置では画像データなどの大量のデータをデスクランブルするのが困難である。

また、ＩＣカード装置のＲＯＭあるいはＥＥＰＲＯＭ内のデータの安全性が問題となる場合、すなわち技術の進歩によりメモリ内のデータの読み出しが可能となった場合、前記従来の技術で示したＩＣカード装置は必ずしも安全な媒体とはならない。

本発明はかかる点に鑑み、ＩＣカード装置内の機密情報を完全に保護し、このＩＣカード装置を用いた簡単な構成のデータ受信装置を提供することを目的とする。

課題を解決するための手段

本発明は上記目的を達成するために、プログラムに従って命令を実行するＣＰＵと、外部からのコマンドに従った処理を行うためのプログラムを格納するＲＯＭと、機密情報を格納するＲＡＭと、前記ＲＡＭ内のデータを保持するための電源を供給する補助電源と、不正行為が行われた場合に前記ＲＡＭへの電源の供給を停止する電源供給遮断手段とを有するＩＣカード装置である。

またこのＩＣカード装置が接続された受信装置であって、受信したデータを機密データと通信相手に伝達すべき所望の伝送データとに分割するデータ分割部と、前記機密データから解読鍵を生成する復号部と、前記復号部を作動させるためのマスター鍵を格納している鍵格納部と、生成された解読鍵を用いて前記伝送データをデスクランブルするデスクランブル部とから構成され、少なくとも前記鍵格納部が前記ＩＣカード装置上に存在することを特徴とする受信装置である。

作用

上記した構成により、このＩＣカード装置に、暗号解読や複製を作成することを目的として、分解をしようとした場合には、電源供給遮断手段が作動してＲＡＭへの電源供給を断ち、ＲＡＭ内に記憶している機密情報を消滅させる。

また、このＩＣカード装置を接続した受信装置においては、デスクランブラ則はＩＣカード装置内には持たず、受信装置本体側に持たせ、ＩＣカード装置にはデスクランブルするためのパラメータを復号する機能を設けたのみであり、簡略化される。

そして、このＩＣカード装置は、受信装置本体と自在に接続及び切り離しが行え、このＩＣカード装置を切り離すと受信またはデスクランブルが行うことができない。

実施例

以下、本発明の一実施例について図面を参照しながら説明する。

第１図は、本発明のＩＣカード装置の構成を示した図である。

ＩＣカード装置１００において、補助電源１４０によってデータを保持できるＲＡＭ１３４はマスター鍵などの機密情報を格納し、ＲＡＭ１３３はプログラムの実行時の作業領域等に使用される。

ＩＣカード装置１００は、入出力部１２０から得たコマンドを解析するプログラムあるいはシステムプログラムなどを格納するＲＯＭ１３１あるいはＥＥＰＲＯＭ１３２と、これらプログラムを実行する中央演算部１１０とを有している。

第２図は、本発明のＩＣカード装置を用いた受信装置の構成図である。ＩＣカード装置２３０において、鍵格納部２３４は第１図のＲＡＭ１３４に相当し、制御部２３２および復号部２３３は第１図のＲＯＭ１３１に相当し、これらの一連の流れを中央演算部１１０が制御し、処理がなされる。

受信装置２００は放送データを受信し分割部２１０へ引き渡す。分割部２１０はこのデータを機密データ２５０と通信相手に伝えたい所望の伝送データ２６０とに分割する。この機密データ２５０はデスクランブルするための鍵パラメータであり暗号化されており、ＩＣカード装置２３０に送信される。伝送データ２６０はデスクランブル部２２０に送信され、解読される。制御部２３２は入出力部２３１を通して得られた暗号化された鍵パラメータを復号部２３３に引き渡し、暗号化された鍵パラメータを復号することのできるマスター鍵が格納されている鍵格納部２３４を制御する。復号部２３３は制御部２３２からの暗号化された鍵パラメータと鍵格納部２３４から引き出したマスター鍵を用いて、伝送データ２６０をデスクランブルするための鍵パラメータを復号する。また入出力部２３１は復号部からの鍵パラメータ２７０を受信装置２００のデスクランブラル部２２０に送信する。デスクランブル部２２０はこの鍵パラメータ２７０をもとに伝送データをデスクランブラし最終出力する。

本発明のＩＣカード装置２３０では、デスクランブラ則２２０に用いる鍵を復号するための機密情報はＲＡＭ１３３に格納されており不正行為によってＲＡＭ１３３への電源供給が停止しするため、機密が守られる。

次に、不正行為等が行われた場合にＲＡＭへの電源供給をストップする電源供給遮断手段について説明する。

第４図は本願発明の電源供給遮断手段の実施例を示したものである。

まず、第４図（ａ）において、４１０は中央演算部１１０、ＲＯＭ１３１、ＥＥＰＲＯＭ１３２、ＲＡＭ１３３及びＲＡＭ１３４が搭載された１チップのＬＳＩである。このＬＳＩ４１０は、同図に示すように、ＩＣカード装置１００内部に埋め込まれており、外観からはＬＳＩ４１０の存在位置はわからないようになっている。１４０は第１図に示すものと同じものでＲＡＭ１３４へ電源を供給する補助電源である。４２０は電源供給遮断手段であり、補助電源１４０からＬＳＩ４１０内のＲＡＭ１３４に電源を供給するリード線で構成されている。同図に示すように、このリード線は補助電源１４０から出発して、ＩＣカード装置１００の内部を張り巡らすようにしたのち、電源供給先であるＲＡＭ１３４に接続されている。そして、第３者が複製あるいは暗号解析等の不正な目的で、ＬＳＩ４１０を取り出そうとした場合はこのリード線を切断してしまい、ＲＡＭ１３４への電源供給が断たれ、機密情報は消滅する。

なお、このリード線の引き回しの方法は、第４図（ａ）のようなものだけではなく、例えば第４図（ｂ）に示すように、ＩＣカード装置１００の厚み方向に対して波状に引き回すことも容易に実現できる。また、第４図（ｃ）に示すようにＩＣカード装置の内部を隙間なくきめ細かに網羅するように配線してもよい。このように配線の方法を複雑にすることで微細な不正行為に対しても電源を遮断することができる。

さらに、本実施例の受信装置２００を用いた放送受信方式では、デスクランブル部２２０を公開することも可能であり、ＩＣカード装置２３０の信頼性は本発明により著しく向上するので、契約者に限定した通信を確実に行うことができる。

このように本実施例によれば、ＩＣカード装置１００自体の安全性が著しく向上するので、このＩＣカード装置１００を用いた受信装置２００においては、たとえ受信装置２００のデスクラブル部２２０に入る復号化された鍵パラメータ２７０が盗聴されたとしても、この鍵パラメータ２７０は短い間隔で更新されていくため、衛生放送などの多量の情報をリアルタイムで処理する不正行為は不可能となる。

発明の効果

以上のように本発明によれば、ICカード装置内の機密情報はRAMに格納されており不正行為によってRAMへの電源供給が遮断されるため機密情報が守られる。

また、このICカード装置を用いた受信装置においては、デスクラブル部に入る鍵パラメータを盗聴したとしても、鍵パラメータは短い間隔で更新されていくため、多量の情報をリアルタイムで処理する不正行為は不可能となる。

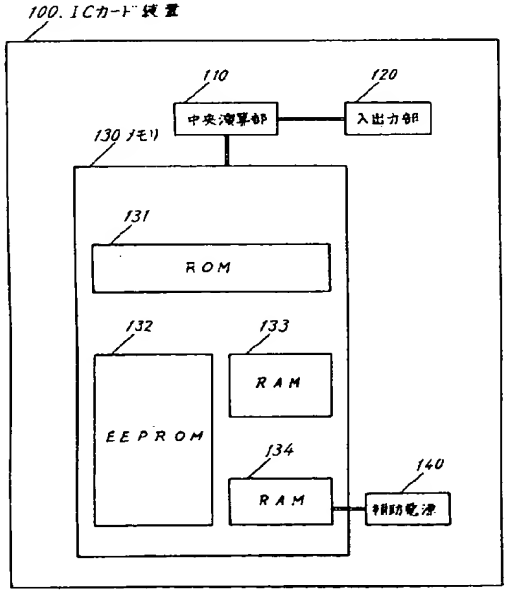
4. 図面の簡単な説明

第1図は本発明のICカード装置の構成図、第2図は本発明のICカード装置を用いた受信装置の構成図、第3図は従来技術のICカード装置を用いた受信装置の構成図、第4図は本発明の電源供給遮断手段の一実施例を示す図である。

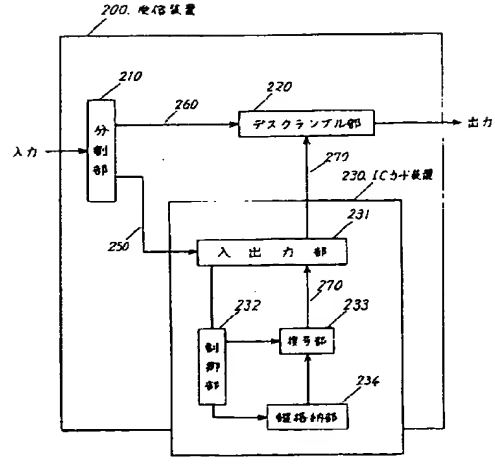
100・・ICカード装置、110・・・中央演算部、131・・・ROM、132・・・EEPROM、134・・・RAM、140・・補助電源、200・・受信装置、220・・デスクランブル部、410・・・LSI、420・・・電源供給遮断手段。

代理人の氏名　弁理士　小鍜治　明　ほか2名

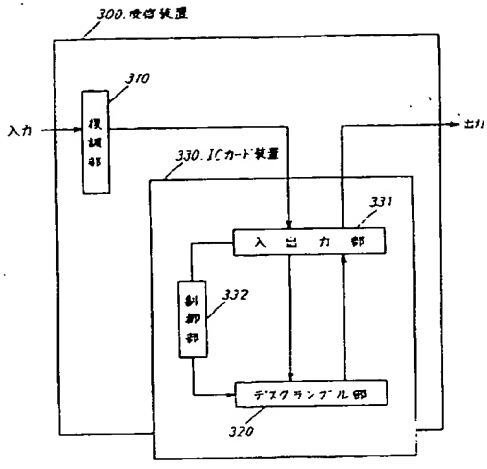
第1図



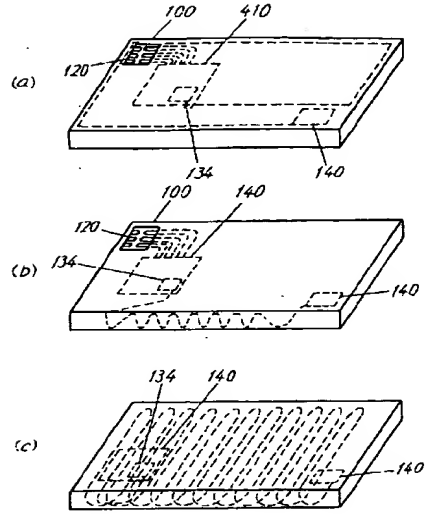
第2図



第 3 図


300.
310
入力
出力
330. ICカード装置
331
入 出 力 部
332
制御部
320

第 4 図


100
410
120
(a)
134
140
100
140
120
(b)
134
140
134
140
(c)
140